ABSTRACT

A copy protection method and a copy protection system are disclosed. The system includes a private key verifier receiving a media certificate that includes a private-key identification of a compliant playing device and searching for an actual private key by checking whether each of available private keys of the playing device corresponds to the private-key identification, a media key decryptor receiving an encrypted media key and decrypting the media key with the actual private key, and a media data decryptor receiving an encrypted media data set and decrypting the media data set with the decrypted media key. The method and system of the present invention are applicable to all types of digital media data, and it makes no assumption of any specific media properties. The primary goal of the present invention is to significantly reduce the possibility of making any illegal copies on any nonstandard equipment and is to restrict the media data transfers only to authorized entities.